CSC-EPL-87/008 (a

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT OF KEY CONCEPTS, INC.

SUREKEY

4 September 1987

Approved For Public Release:
Distribution Unlimited

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No 0704-0188

1a REPORT SECURITY CLASSIFICATION
UNCLASSIFIED

1b RESTRICTIVE MARKINGS
NONE

2a SECURITY CLASSIFICATION AUTHORITY

2b DECLASSIFICATION / DOWNGRADING SCHEDULE

3 DISTRIBUTION / AVAILABILITY OF REPORT
DISTRIBUTION UNLIMITED

4 PERFORMING ORGANIZATION REPORT NUMBER(S)
CSC-EPL-87/008

5 MONITORING ORGANIZATION REPORT NUMBER(S)
S228,577

6a NAME OF PERFORMING ORGANIZATION
National Computer Security Center

6b OFFICE SYMBOL (If applicable)
C12

7a NAME OF MONITORING ORGANIZATION

6c ADDRESS (City, State, and ZIP Code)
9800 Savage Road
Ft. George G. Meade, MD 20755-6000

7b ADDRESS (City, State, and ZIP Code)

8a NAME OF FUNDING / SPONSORING ORGANIZATION

8b OFFICE SYMBOL (If applicable)

9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c ADDRESS (City, State, and ZIP Code)

10 SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO	PROJECT NO	TASK NO	WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification)
(U) Sub-system Evaluation Report, Key Concepts, Inc. SureKey

12 PERSONAL AUTHOR(S)
Leon Neufeld, Rick Siebenaler

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Final	FROM ________ TO ______	4 September 1987	18

16 SUPPLEMENTARY NOTATION

17 COSATI CODES

FIELD	GROUP	SUB-GROUP

18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
NCSC; TCSEC; sub-system; Key Concepts, Inc; SureKey; Authentication; (KT)

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

The Key Concpets, Inc. SureKey product was evaluated against identification and authentication requirements of the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), dated December 1985. The product is an IBM PC/XT hardware/software package which, when properly installed, provides user authentication.

This report documents the findings of the evaluation. keywords: computer security; test and evaluation; computer program;

20 DISTRIBUTION / AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS

21 ABSTRACT SECURITY CLASSIFICATION
UNCLASSIFIED

22a NAME OF RESPONSIBLE INDIVIDUAL	22b TELEPHONE (Include Area Code)	22c OFFICE SYMBOL
LTC Lloyd D. Gary, USA	(301)859-4458	C/C12

Previous editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED

SUBSYSTEM EVALUATION REPORT

KEY CONCEPTS, INC.

SUREKEY

NATIONAL
COMPUTER SECURITY CENTER

9800 SAVAGE ROAD
FORT GEORGE G. MEADE
MARYLAND 20755-6000

September 4, 1987

CSC-EPL-87/008
Library No. S228,577

This page intentionally left blank.

CSC-EPL-87/008
Library No. S228,577

FOREWORD

This publication, the Subsystem Evaluation Report of Key Concepts, Inc., SureKey, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document the results of an evaluation of Key Concepts' product SureKey.

Approved:

September 4, 1987

Eliot Sohmer
Chief, Product Evaluations and Technical Guidelines
National Computer Security Center

ACKNOWLEDGEMENTS

Team Members

Leon Neufeld
Rick Siebenaler

National Computer Security Center
9800 Savage Road
Fort George G. Meade, Maryland

Further Acknowledgements

Technical support was also provided by Cornelius J. Haley.

CONTENTS

This page intentionally left blank.

EXECUTIVE SUMMARY

The Key Concepts, Inc., SureKey system has been evaluated by the National Computer Security Center (NCSC). SureKey is considered to be a security subsystem rather than a complete trusted computer system, therefore it was evaluated against a relevant subset of the requirements from the DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (Criteria). The identification and authentication requirement is the most relevant, and as such it was used as an evaluation metric. Additionally, SureKey is designed to allow a user to lock the system keyboard.

The NCSC evaluation team has determined that SureKey is capable of providing minimal user authentication when installed within an IBM PC XT. SureKey authenticates potential users by requiring each user to enter a valid password prior to granting access to the system. In the case of the SureKey administrator, after password authentication he she has access to system maintenance menus. The authentication process required by SureKey provides some assurance to the system administrator that only authorized persons can use the system.

SureKey is also designed to allow an authenticated user the ability to lock the system keyboard. SureKey can also be set to lock the keyboard if text has not been entered for a prespecified period of time.

These security mechanisms can be maintained only if SureKey's integrated hardware is protected from physical tampering. Since SureKey is installed within an IBM PC/XT, some means to physically secure the PC should be employed. In addition, the System Administrator should determine that none of the other Read-Only Memory based products (i.e., serial cards, printer cards, drive controller cards, etc.) used in the system interact with SureKey.

This page intentionally left blank.

INTRODUCTION

Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center (DoDCSC) was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September 1984, National Security Decision Directive 145 (NSDD 145) expanded these responsibilities to include all federal government agencies. At that time the Center became known as the National Computer Security Center (NCSC).

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems; that is, systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information. Such encouragement is brought about by evaluating the technical protection capabilities of industry and government developed systems, advising system developers and managers of their systems' suitability for use in processing sensitive information, and assisting in the incorporation of computer security requirements in the systems acquisition process.

The NCSC Computer Security Subsystem Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multipurpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Computer Security Subsystem Evaluation Program.

The goal of the NCSC's Computer Security Subsystem Evaluation Program is to provide computer installation managers with information on subsystems that may be helpful in providing immediate computer security improvements to existing installations.

Introduction

Subsystems considered in the program are special-purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of government departments and agencies. For the most part, the scope of a computer security subsystem evaluation is limited to consideration of the subsystem itself, and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations, and where appropriate, an attempt is made to assess a subsystem's security relevant performance in light of applicable standards and features outlined in the Criteria. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of the evaluation report will be placed on the Evaluated Products List.

The report will not assign a specific rating to the product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security.

PRODUCT EVALUATION

Product Overview

The SureKey system is an integrated hardware device which provides minimal system access control for an IBM PC/XT.

The SureKey system consists of a plug-in card which is inserted into the BASIC ROM socket on an IBM PC XT system board. The location of this socket is such that installation of SureKey does not reduce the availability of system bus expansion slots. Because of the initialization process of an IBM PC/XT, SureKey's correct operation could be subverted if another product assumed control of the system. Because of this, the System Administrator should determine that no other ROM-based expansion cards interact with SureKey.

Five user passwords and a system administrator password are defined to the SureKey system. These six passwords are used to authenticate potential users of the system. SureKey also provides a method with which an authenticated user can lock the system keyboard.

When the system is powered up, SureKey forces all potential users to enter a valid password before allowing access to the protected system. After granting access to the system, SureKey monitors keystrokes to detect the entry of a keyboard lock sequence. If the keyboard lock sequence is entered or a prespecified time elapses between keystrokes, SureKey will prevent further information from being entered through the keyboard. Only after the password of the current user is entered or the system is powered down, can the keyboard lock be reset.

Evaluation of Functionality

The SureKey system provides a limited increase in assurance that the user of the protected system is authorized. SureKey requires only the entry of a valid authentication string, password, before allowing access to the protected system. Access control, as implemented by SureKey, is not complete in that it does not require both identification and authentication. A person attempting to access the system need enter only one of six authentication passwords.

Before gaining access to an IBM PC/XT protected by SureKey, each potential user must enter one of the valid passwords, as established by the system administrator. There are two classes of passwords, user and administrator. When a valid user password is entered, the system continues normal boot-up processing and is available for use. When the administrator password is entered, a menu is displayed which allows the display and modification of user/administrator passwords and the control of the keyboard locking features.

Five user passwords as well as the administrator password are defined by SureKey. Entering any of the five user passwords affords the same access to the information contained within the system. Entering the system administrator affords access to the administrator functions and all system passwords, as well as access to the information contained within the system. Valid passwords are from three to eight upper case characters or numbers. Lower case characters are automatically converted into upper case.

SureKey allows two invalid access attempts before locking the system. After a lockup condition, the system can only be brought back online through a cold boot. This retards password guessing attacks because of time needed for the reboot. SureKey does not provide any mechanism to detect that a series of password guessing attacks have been made.

SureKey uses a non-volatile memory chip and supporting hardware logic to store passwords. The hardware logic allows SureKey to read and write to the non-volatile memory during password verification and then to disable access to the password storage area during normal operations.

Although SureKey offers only a minimal increase in assurance, the NCSC feels that the product could be useful in some environmerts.

Evaluation of Documentation

The SureKey system is delivered with a single documentation package that can be logically separated into a user's guide and an installation guide

The user's guide is a one-page document that provides a description of the features of SureKey. It discusses the system access and keyboard locking mechanisms. The installation guide is a two-page document that accurately describes the proper installation procedure for SureKey. Several drawings are included to facilitate installation. The administrator password is also given here, and as such it is imperative that the SureKey administrator changes the password upon initial system startup.

This page intentionally left blank.

THE PRODUCT IN A TRUSTED ENVIRONMENT

The rapid introduction of office automation products into the workplace has brought with it the need to protect and control access to the data stored on these systems. It is now common practice to have many users sharing the same system. Many office automation systems maintain little or no means to restrict unauthorized users from accessing these systems. Without the use of a user identification and authentication mechanism to restrict access to these systems, there cannot be any assurances that the data residing on them is protected from unauthorized disclosure or modification.

Many environments require more than one person to have access to the system, and yet still prevent access to people outside the select group. The use of physical means such as keys to maintain this separation would be awkward and hard to control at best. An electronic locking mechanism would be more suited for this type of access control. In this type of environment, SureKey could be used to provide such a separation. SureKey's user authentication mechanism provides an increased assurance that system users are those who are authorized access to the information maintained by the system. The keyboard lock feature also provides a method with which users can easily secure the system when leaving it momentarily unattended.

This page intentionally left blank.

PRODUCT TESTING

Test Procedure

Testing represents a significant portion of a subsystem evaluation. The test suite used by the evaluation team tested SureKey's identification and authentication mechanism, verified the correct operation of the administrator functions, and attempted to read the access control information (passwords and code) used by SureKey. The test suite consisted of password guessing attacks, where unauthorized persons entered combinations of alphanumeric characters at the logon prompt in an attempt to enter the system. The administrator also attempted to assign invalid passwords (e.g., passwords less than three or more than eight characters).

All tests were performed using an IBM PC/XT using DOS 3.1, a multi-I/O card with 2 serial ports and 1 parallel port, a color graphics adapter card, and floppy disk drive and hard disk drive controllers. SureKey was installed as described in the system documentation. The System Administrator set all passwords to 8 characters in length.

When SureKey is installed, some form of physical security should be employed to provide some assurances that the product will not be removed from the system. Since SureKey is not integrated into the system code, it would be possible for an unauthorized user to remove the product and access the system without being detected.

Test Results

Identification and Authentication

SureKey was found to provide a limited increase in assurance that system users are authorized. Access control, as implemented by SureKey, is not complete in that it provides only authentication and not identification.

It was found that SureKey allows access to a protected system only when one of the six (five user and one administrator) valid passwords is entered.

After two invalid access attempts, SureKey locks the system such that a cold boot is required for restart.

System Administrator Function Tests

SureKey provides an extensive menu system to perform system administrative functions. Through the menu system, the administrator is able to display and modify the user and administrator passwords as well as update the status of the keyboard locking mechanisms.

The menu system did not allow the system administrator to enter passwords of less than three or greater than eight alpha-numeric characters. A thorough test of the menu functions produced the correct and expected results.

Search for Obvious Flaws

After examining SureKey's design documentation, the team attempted to access password information by executing SureKey's code at various non-standard entry points.

It was found that the design and implementation properly maintained the integrity of SureKey's password information.